STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1955-017/2

On theorems of Wolstenholme and Leudesdorf

Additional note

H.J.A. Duparc and W. Peremans

1955

ZW

KONINKL. NEDERL. AKADEMIE VAN WETENSCHAPPEN - AMSTERDAM
Reprinted from Proceedings, Series A, 59, No. 1 and Indag. Math., 18, No. 1, 1956

MATHEMATICS

ON THEOREMS OF WOLSTENHOLME AND LEUDESDORF
ADDITIONAL NOTE

BY

H. J. A. DUPARC AND W. PEREMANS

(Communicated by Prof. J. F. KOKSMA at the meeting of September 24, 1955)

To our paper "On theorems of WOLSTENHOLME and LEUDESDORF" [1] we want to add two additional remarks.

I. First we want to prove the following extension of theorem 2 of our paper [1]:

Theorem 3. If M is a positive integer, if p is a prime and n a positive integer such that $p^n \,||\, M$, if e is a non-negative integer such that $p^e \mid \varphi(Mp^{-n})$, if s is an integer and if k is the exponent introduced in theorem 1 of [1], then $p^{k+e} \mid T_s(M)$.

Proof: We use mathematical induction with respect to the number of different prime factors of Mp^{-n}. If this number is zero, we have $e=0$ and $M=p^n$; the theorem then follows from theorem 1 of [1].

Now put $M=q^r m$, q being a prime different from p, $(m,q)=1$ and $r \geqq 1$. We may put $e=e_1+e_2$, $p^{e_1} \mid q-1$, $p^{e_2} \mid \varphi(mp^{-n})$. We may suppose $p^{k+e_2} \mid T_s(m)$ for all integers s and corresponding k.

We have

$$T_s(M) = \sum_{a=1}^{m}{}' \sum_{v=0}^{q^r-1} (a+vm)^{-s} - q^{-s} \sum_{a=1}^{m}{}' \sum_{v=0}^{q^{r-1}-1} (a+vm)^{-s}.$$

For sufficiently large l we have $p^{k+e} \mid m^l$; by lemma 1 of [1] we have

$$\sum_{a=1}^{m}{}' (a+vm)^{-s} \equiv \sum_{a=1}^{m}{}' \sum_{h=0}^{l-1} \binom{-s}{h} a^{-s-h} v^h m^h =$$

$$= \sum_{h=0}^{l-1} \binom{-s}{h} v^h m^h T_{s+h}(m) \pmod{p^{k+e}},$$

so

$$T_s(M) \equiv \sum_{h=0}^{l-1} \binom{-s}{h} m^h T_{s+h}(m) \left\{ \sum_{v=0}^{q^r-1} v^h - q^{-s} \sum_{v=0}^{q^{r-1}-1} v^h \right\} \pmod{p^{k+e}}.$$

It is well-known that $\sum_{v=0}^{u-1} v^h = \frac{1}{r_h} P_h(u)$, where $P_h(x)$ is a polynomial in x with integral coefficients, whereas $r_0=1$, $r_1=2$, $r_2=6$, $r_3=4$, and r_h is a positive integer dividing $(h+1)!$ for every integer $h \geqq 0$ [1]). Furthermore

$$P_h(x^r) - x^{-s} P_h(x^{r-1}) = (x-1)\, x^{-|s|} Q_h(x),$$

[1]) Using the theorem of VON STAUDT-CLAUSEN one could get a sharper result. The statement given by us, which may be obtained by elementary means, suffices for our purpose.

where Q_h is a polynomial with integral coefficients. So we get

$$T_s(M) \equiv \sum_{h=0}^{l-1} \tau_h \pmod{p^{k+e}},$$

where

$$\tau_h = \binom{-s}{h} m^h T_{s+h}(m) \frac{1}{r_h} q^{-|s|}(q-1) Q_h(q).$$

We are going to prove that for $h=0, 1, \ldots$ the number of factors p in τ_h is $\geqq k+e$.

Now we use the fact that the number of factors p in $(h+1)!$ is $\leqq \dfrac{h}{p-1}$. In fact let the integer t be chosen such that $p^t \leqq h+1 < p^{t+1}$. Then that number is equal to

$$\left[\frac{h+1}{p}\right]+\left[\frac{h+1}{p^2}\right]+\ldots+\left[\frac{h+1}{p^t}\right] \leqq \frac{h+1}{p} + \ldots \frac{h+1}{p^t} =$$
$$= \frac{h+1}{p-1}\left(1-\frac{1}{p^t}\right) \leqq \frac{h+1}{p-1}\left(1-\frac{1}{h+1}\right) = \frac{h}{p-1}.$$

If k' is the number for which, according to theorem 1 of [1], $p^{k'} \mid T_{s+h}(p^n)$ holds and if g denotes the number of factors p in r_h, the number of factors p in τ_h is $\geqq nh+k'+e_2-g+e_1$. In order to prove that this number is $\geqq k+e$, it suffices to prove $\alpha = nh+k'-k-g \geqq 0$.

From theorem 1 of [1] it follows that in general we have $k'-k \geqq -n-1$; if $p=2$ we have $k'-k \geqq -n+1$; if h is even we have $k'-k \geqq -1$.

First suppose $p=2$. We then have $g \leqq h$, and $\alpha \geqq nh-n+1-h = (n-1)(h-1)$, which is $\geqq 0$ for $h \geqq 1$.

Now suppose $p \geqq 3$. We then have $g \leqq \frac{1}{2}h$, and $\alpha \geqq nh-n-1-\frac{1}{2}h = \frac{1}{2}(h(2n-1)-2n-2)$, which is $\geqq 0$ for $h \geqq 4$. For $h=3$ we have $g=0$, and $\alpha \geqq 2n-1 \geqq 0$. For $h=2$ we have $g \leqq 1$, and $\alpha \geqq 2n-2 \geqq 0$.

We are left with the cases $h=0$ and $h=1$, $p \geqq 3$.

If $h=0$, we have $k'=k$ and $g=0$, so $\alpha \geqq 0$.

If $h=1$, $p \geqq 3$, we have $g=0$, and $\alpha = n+k'-k$. The only case in which this is <0, is $k=2n$, $k'=n-1$; this occurs if $2 \nmid s$, $p \mid s$, $p-1 \mid s+1$. But in this case $\binom{-s}{1} = -s$ has a factor p. Consequently we may infer that also here the number of factors p in τ_1 is $\geqq k+e$. This completes the proof of our theorem.

Remark 1. It is possible to determine in some cases the exact number of factors p in $T_s(M)$. We shall not enter into this detail.

Remark 2. As theorem 2 of [1] is not used in the proof of theorem 3, the above result furnishes a new proof of theorem 2a) and 2c) of [1].

II. Further we want to give a short discussion of the results of N. ELJOSEPH [2], [3], which came to our knowledge only after correcting the revision of our paper [1]. See the concluding "Note on two papers of ELJOSEPH" in [1].

First we mention the fact that our theorems 1 and 2 of [1] are included in his. Moreover he proves a theorem, which in our notation, reads as follows:

If for all prime factors p of M one has $p-1 \mid s$, then

$$T_s(M) \equiv \varphi(M) \pmod{M},$$

except if s is odd and $M = 2^n$ with $n \geqq 2$.

Using the ideas of our proofs of the theorems 1 and 2 of [1] it is not difficult to give a new proof of this theorem.

In [2] ELJOSEPH gives his proofs by making use of the theorem of VON STAUDT–CLAUSEN on BERNOULLI numbers. It has to be remarked that in [2] formula (9) is wrong. In the righthand side a term

$$\sum_{j=1}^{k} \binom{k}{j} m_1^j T_{k-j}(m_1)(p^j - p^k) \sum_{l=1}^{p^{e-1}-1} l^j$$

has to be added. However this term, although in general not equal to zero, happens to be congruent 0 mod p^e (this follows immediately from the fact that $p^{e-1} \mid \sum_{l=1}^{p^{e-1}-1} l^j$), which is sufficient for ELJOSEPH's purpose.

In our paper [1] we have avoided on purpose the use of this less elementary theorem of VON STAUDT–CLAUSEN. In [3] also ELJOSEPH wants to eliminate the use of VON STAUDT–CLAUSEN in the proofs of his results. Unfortunately however his proof in § 6 is erroneous, the assertion that for $k = (p-1)p^s u$ (where $0 \leq s < \frac{1}{2}(e-1)$ and $p \nmid u$) the expression $k' = \varphi(p^e) - k$ contains at least $\frac{1}{2}(e-1)$ factors p being wrong. At this moment we do not see how this second method of ELJOSEPH may lead to a correct proof.

REFERENCES

1. DUPARC, H. J. A. and W. PEREMANS, On theorems of Wolstenholme and Leudesdorf, Proc. Kon. Ned. Ak. v. Wetensch. **A 58**, 459–465 (1955).
2. ELJOSEPH, N., Extensions of Wolstenholme's theorem, Riv. Lemat. **4**, 9–15 (1950).
3. ———, Remarks on my paper "Extensions of Wolstenholme's theorem", Riv. Lemat. **4**, 59–61 (1950).